Урок № 9

Тема. Контроль цілісності програмних і інформаційних ресурсів. Виявлення атак. Захист периметра комп'ютерних мереж. Керування механізмами захисту. Міжнародні стандарти інформаційної безпеки.

**Мета:**

* ***навчальна:*** дати уявлення про захист комп'ютерних мереж, про міжнародні стандарти інформаційної безпеки;
* ***розвиваюча:*** розвивати логічне й алгоритмічне мислення; формувати вміння діяти за інструкцією, планувати свою діяльність, аналізувати i робити висновки;
* ***виховна:*** виховувати інформаційну культуру учнів, уважність, акуратність, дисциплінованість, виховання уміння працювати в групі; формування позитивного ставлення до навчання

**Обладнання:** комп’ютери кабінету з виходом в мережу Інтернет, мультимедійний проектор, презентація уроку, електронні матеріали.

**Тип уроку:** урок засвоєння нового матеріалу.

**ХІД УРОКУ.**

**І. Організація класу до уроку**

**II. Перевірка домашнього завдання. Актуалізація опорних знань**

1. Комп’ютерне тестування– Урок 8 (Mytest)

**Мотивація навчання**

Мережнi й iнформацiйнi технологiї мiняються настiльки швидко, що статичнi захиснi механiзми, до яких відносяться й системи розмежування доступу, i системи автентифiкацiї, сильно обмеженi й у багатьох випадках не можуть забезпечити ефективного захисту. Тому потрiбнi динамiчнi методи, що дозволяють оперативно виявляти й запобiгати порушення безпеки. Однiєї з технологiй, що дозволяє виявляти порушення, якi не можуть бути iдентифiкованi за допомогою традицiйних моделей контролю доступу, є технологiя виявлення атак.

IV. Вивчення нового матеріалу

**Пояснення вчителя з елементами демонстрування презентації**

*(використовується проектор)*

 Цілісність є однією з властивостей безпеки інформації. Цілісність забезпечується або механізмами розмежування доступу, або механізмами контролю цілісності.

Під *контролем цілісності інформації* розуміють процес перевірки наявності викривлень цієї інформації, незалежно від причин їх походження (навмисні чи ненавмисні)

Під *контролем та поновленням цілісності інформації* розуміють процес перевірки наявності викривлень цієї інформації, незалежно від причин їх походження (навмисні чи ненавмисні), з наступною корекцією викривленої інформації.

Порушення цілісності може статись в наслідок наступних причин:

1. помилок користувачів, які викликають викривлення чи втрату інформації;
2. навмисних дій осіб, які не мають прав доступу до  автоматизованої системи;
3. збоїв обладнання, які викликають викривлення чи втрату інформації;
4. фізичних впливів на носії інформації;
5. вірусних впливів.

Цілісність програмних засобів та інформації, що обробляється досягається використанням двох груп механізмів захисту - без перетворення інформації та механізмів захисту з її перетворенням.

До механізмів забезпечення цілісності без перетворення інформації слід віднести використання резервних копій програмних засобів та баз даних. Такий спосіб, безумовно, є найнадійнішим, оскільки завжди дозволяє не тільки установити факт порушення цілісності, але й поновити порушену інформацію, правда це є і першою вадою. Іншими словами, цей спосіб не дає змоги оперативно установити наявність порушення цілісності інформації, що змінюється.

До другої групи механізмів захисту  відносяться такі відомі механізми з використанням: сигнатур важливих об’єктів, хеш – функції важливих об’єктів, забезпечення цілісності архівної інформації в тому числі і резервних копій програмних засобів та баз даних.

При передачі інформації по каналах зв’язку контроль цілісності (контроль наявності будь – яких викривлень інформації) та усунення цих викривлень покладаються на комунікаційне обладнання та протоколи зв’язку. Проблема поновлення цілісності вирішується за рахунок повторної передачі повідомлень Таким чином, механізми захисту з використанням сигнатур важливих об’єктів ґрунтуються на застосуванні швидко діючих процедур виявлення порушення цілісності та подальшому поновленні викривленої інформації за рахунок повторної передачі непошкодженої інформації чи повторного запису непошкодженої інформації з її резервної копії.

Механізми захисту з використанням хеш: контроль цілісності інформації носія забезпечується шляхом порівняння хеш функції відповідного носія, яка обчислюється під час контролю цілісності інформації, з хеш-функцією, яка була обчислена для того ж самого носія під час запису інформації. Якщо ці функції співпадають, то цілісність даного носія не порушена.

**Виявлення атак. Захист периметра комп’ютерних мереж**

Процес виявлення атак є процесом оцiнки пiдозрiлих дiй, якi вiдбуваються в корпоративнiй мережi. Iнакше кажучи, виявлення атак (intrusion detection) це процес iдентифiкацiї й реагування на пiдозрiлу дiяльнiсть, спрямовану на обчислювальнi або мережнi ресурси.

Основні підходи до [виявлення атак](http://easy-code.com.ua/2010/12/viyavlennya-bezdrotovix-atak/) практично не змінилися за останню чверть століття, і, незважаючи на гучні заяви розробників, можна з упевненістю стверджувати, що [виявлення атак](http://easy-code.com.ua/2012/09/viyavlennya-bezdrotovix-atak-kriptografiya-security-hack-statti/) базується або на методах *сигнатурного аналізу*, або на методах *виявлення аномалій*. Можливо також спільне використання зазначених вище методів.

Iснує кiлька способiв класифiкацiї систем виявлення атак, кожен з яких заснований на рiзних характеристиках:

* *Спосiб контролю за системою* (подiляються на network-based, host-based i applicationbased).
* *Спосiб аналiзу.* (частина системи визначення проникнення, яка аналiзує подiї, отриманi з джерела інформації, i приймає рiшення, чи вiдбувається проникнення). Способами аналiзу є виявлення зловживань (misuse detection) та виявлення аномалiй (anomaly detection).
* *Затримка в часi мiж отриманням iнформацiї з джерела та її аналiзом i прийняттям рiшення*. Залежно вiд затримки в часi, системи виявлення атак дiляться на interval-based (або пакетний режим) i real-time.

Механiзми виявлення атак, застосовуванi в сучасних системах виявлення атак IDS (Intrusion Detection System), заснованi на декiлькох загальних методах.

Класифiкацiя систем виявлення атак може бути виконана за декiлькома ознаками:

* *за способом реагування*; розрiзняють пасивнi й активнi IDS. **Пасивнi** IDS просто фiксують факт атаки, записують данi у файл журналу й видають попередження. **Активнi** IDS намагаються протидiяти атацi.
* за способом виявлення атаки; За способом виявлення атаки системи IDS прийнято дiлити на двi категорiї: *виявлення аномального поводження* (anomaly-based); *виявлення зловживань* (misuse detection або signature-based). Аномальне поводження користувача (тобто атака або яка-небудь ворожа дiя) часте проявляється як вiдхилення вiд нормального поводження. Прикладом аномального поводження може служити велика кiлькiсть з’єднань за короткий промiжок часу, високе завантаження центрального процесора й т.iн. Однак аномальне поводження не завжди є атакою. Наприклад, одночасну посилку великої кiлькостi запитiв вiд адмiнiстратора мережi система виявлення атак може iдентифiкувати як атаку типу “вiдмова в обслуговуваннi” (denial of service).
* *за способом збору iнформацiї про атаку*.

**Аналіз активності**

#### Статичні і динамічні IDS

* Статичні засоби роблять «знімки» (snapshot) середовища та здійснюють їх аналіз, розшукуючи вразливе ПО, помилки в конфігураціях і т. д. Статичні IDS перевіряють версії прикладних програм на наявність відомих вразливостей і слабких паролів, перевіряють вміст спеціальних файлів в директоріях користувачів або перевіряють конфігурацію відкритих мережевих сервісів. Статичні IDS виявляють сліди вторгнення.
* Динамічні IDS здійснюють моніторинг у реальному часі всіх дій, що відбуваються в системі, переглядаючи файли аудиту або мережні пакети, що передаються за певний проміжок часу. Динамічні IDS реалізують аналіз в реальному часі і дозволяють постійно стежити за безпекою системи.

#### Мережеві IDS

* Мережеві IDS ([англ.](https://uk.wikipedia.org/wiki/%D0%90%D0%BD%D0%B3%D0%BB%D1%96%D0%B9%D1%81%D1%8C%D0%BA%D0%B0_%D0%BC%D0%BE%D0%B2%D0%B0) *Network-based IDS, NIDS*) розташовуються в стратегічному місці або у таких місцях мережі, де можливий контроль трафіку всіх пристроїв у мережі. Вони здійснюють контроль усього трафіку даних всієї підмережі та порівнюють трафік, який передається у підмережі з бібліотекою відомих атак. Як тільки розпізнана атака або визначено відхилення у поведінці, відразу відсилається попередження адміністратору.

#### Хостові IDS

* IDS, які встановлюються на хості і виявляють зловмисні дії на ньому називаються хостовими або системними IDS.

**Експертнi системи.**

* Експертна система складається з набору правил, якi охоплюють знання людини-експерта. Використання експертних систем являє собою розповсюджений метод виявлення атак, при якому iнформацiя про атаки формулюється у виглядi правил. Цi правила можуть бути записанi, наприклад, у виглядi послiдовностi дiй або сигнатури. При виконаннi кожного iз цих правил приймається рiшення про наявнiсть несанкцiонованої дiяльностi. Важливим достоїнством такого пiдходу є практично повна вiдсутнiсть фiктивних тривог.

Сигнатурний аналіз заснований на припущенні, що сценарій атаки відомий і спроба її реалізації може бути виявлена ​​в журналах реєстрації подій або шляхом аналізу мережевого трафіку

**Стандарти кібербезпеки**

**Стандарти кібербезпеки** – це методи, що зазвичай викладені в опублікованих матеріалах, які намагаються захистити кібернетичне середовище користувача чи організації.

Це середовище включає в себе користувачів, мережі, пристрої, все програмне забезпечення, процеси, інформацію в режимі зберігання або транзиту, програми, служби та системи, які можуть бути безпосередньо або опосередковано підключені до мереж.

**Основна мета** — знизити ризики, включаючи попередження або пом'якшення кібер-атак. Ці опубліковані матеріали включають збірки інструментів, політику, концепції безпеки, гарантії безпеки, керівні принципи, підходи до управління ризиками, дії, навчання, найкращі практики, забезпечення та технології.

**Міжнародні стандарти**

 **BS 7799-1: 2005** — Британський стандарт BS 7799 перша частина. BS 7799 Частина 1 — Кодекс практики управління інформаційною безпекою (Практичні правила управління інформаційної безпеки) описує 127 механізмів контролю, необхідних для побудови системи управління інформаційною безпекою (СУІБ) організації, визначених на основі кращих прикладів світового досвіду в цій області . Цей документ служить практичним керівництвом по створенню СУІБ

**BS 7799-2: 2005** — Британський стандарт BS 7799 друга частина стандарту. BS 7799 Частина 2 — Управління інформаційною безпекою — специфікація систем управління інформаційною безпекою (Специфікація системи управління інформаційної безпеки) визначає специфікацію СУИБ. Втора частина стандарту використовується як критерії при проведенні офіційної процедури сертифікації СУІБ організації.

**BS 7799-3: 2006** — Британський стандарт BS 7799 третя частина стандарту. Новий стандарт в області управління ризиками інформаційної безпеки

**ISO/IEC 17799: 2005** — «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Міжнародний стандарт, базувався на BS 7799-1: 2005.

**ISO/IEC 27000** — Словарь і визначення.

**ISO/IEC 27001** — «Інформаційні технології — Методи забезпечення безпеки — Системы управління інформаційної безпеки — Требования». Міжнародний стандарт, базувався на BS 7799-2: 2005.

**ISO/IEC 27002** — Зараз**: ISO/IEC 17799: 2005**. «Інформаційні технології — Технології безпеки — Практичні правила управління інформаційної безпеки». Дата выхода — 2007 год.

**ISO/IEC 27005** — Зараз: **BS 7799-3: 2006** — Руководство по управлению рисками ИБ.

Німецьке агентство з інформаційної безпеки. Інструкція з захисту базової лінії — стандартні гарантії безпеки (керівництво по базовому рівню захисту інформаційних технологій).

1. Формування практичних умінь і навичок

**Увага! *Під час роботи з комп’ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

# Завдання 1. *Ознайомитися з стандартами інформаційної безпеки, скориставшись Вікіпедією.*

**Завдання 2**. Створити карту знань до уроку

1. Підсумок уроку

**Рефлексія**

* + *Що нового сьогодні дізналися? Чого навчилися?*
	+ *Що сподобалось на уроці, а що ні? Чи виникали труднощі?*
1. **Домашнє завдання**
2. Опрацювати **конспект**,
3. За матеріалами Інтернету підготуйте доповідь «Які є види мережевих атак?». Розмісіть роботу на Google-диску, наддайте доступ, для перегляду і редагування учителю і 2 однокласникам. Перегляньте проектну роботу своїх друзів